January 28, 2002

SEQUOIA
voting systems

Office of Election Administration
Federal Election Commission
Attn: Penelope Bonsall
999 East Street, N.W.
Washington DC, 20463

RE: Sequoia Voting Systems consolidated comments to the second draft of the revisions to the 1990 national voluntary performance standards for computerized voting systems and the first draft of the revisions to the 1990 national test standards.

Dear Penelope:

Please accept the attached document as Sequoia's comments to the revisions of the above proposed standards.

Appreciatively,

Tom Keeling
VP Product Development

7677 Oakport Street, Suite 800
Oakland, CA 94621
t:510.875.1200
t:800.869.1936
f:510.875.1226
www.sequoiavote.com

SEQUOIA
voting systems

January 28, 2002

FEC Draft Voting System Standards

We would like to start by complimenting the committee for their efforts in bringing this standards revision effort to this point. There is much to be proud of in this draft.

That being said, we do wish to raise points, ask questions, and request clarifications, both at a general level and with regard to specific paragraphs.

Our response is divided into three sections. General Comments are first, with higher-level issues and concerns. These are followed by specific notes for volume I and volume II.

General Comments

Internet Voting

As we have studied the revised documents, it has become clear that the treatment of Internet voting has been significantly altered. For example, the original draft of Volume I stated in section 1.5.4:

> *The VSS are defined to apply to each of the Internet Voting System scenarios defined above. Recognizing the risks and research needs cited in studies of Internet voting conducted to date, including the Report of the National Workshop on Internet Voting: Issues and Research Agenda, March 2001 (sponsored by the National Science Foundation), the Standards allow for Internet voting systems operated in parallel with another voting system, and do not allow for a standalone Internet voting system.*

The change in attitude towards Internet voting between the two drafts is surprising. If anything, the security and privacy concerns raised by various investigations into Internet voting are even more valid; indeed, does a week go by without some new failure of popular operating system and Internet software being discovered?

This change between the drafts leads to our second issue:

Revision Control

The FEC must practice what it preaches. In the area of revision control, specific requirements for change notes are delineated in the standards. Yet this revised has nothing of the sort. No markup of changed sections. And most important, no discussion of the reasons for the changes that were made.

SEQUOIA
voting systems

Places where significant changes have been made appear to include:

Internet voting
Accessibility
Deletion of the requirement for a voting booth for DRE systems
Added environmental tests
Detailed software design requirements

Are there others that we have missed?

Without this information it becomes nearly impossible to respond in a coherent fashion, let alone within the shortened comment period.

Existing Systems

There is but one place where the issue of grandfathering existing certified systems is mentioned, in Volume II, Section 2.1.1.1. This section refers to "developmental" documentation, without ever defining what that includes.

Given the number of already certified systems, we strongly urge that the transition to the new standards be addressed. In particular, the following questions:

1. Are existing certified systems brought forward, or must all systems comply with the new standards when they are adopted?
2. If the answer to (1) is that existing systems are brought forward, is there a "sunset" date when they must comply with the new standards?
3. For systems undergoing certification before the revised standards are adopted, that are not completed on the adoption date, shall such certification effort still be subject to the original standards?
4. For a system that is already certified, where a minor change (a simple fix, perhaps) has been made, shall the entirety of the new standards apply? If not, what subset?

Certification Timeframe

Florida's proposed new voting system standards include timeframes for the entire certification process, for example:

> *"Within 10 workdays after completion of all successful qualification testing the Division shall issue a Qualification Test Report which documents the conduct of tests, results of tests and the Division's findings of compliance"*

A similar approach in the FEC standards is recommended to address the historically very long ITA delays.

SEQUOIA
voting systems

Appeals Process

As an established vendor, we have been through the certification process numerous times. We have encountered situations where different ITAs interpret the standards inconsistently. We have also been involved in situations where the ITAs have turned to the NASED technical committee for guidance on an issue.

We have two recommendations to make on the above:

1. That the existing informal appeals process to NASED's technical committee be codified in the standards, *including an opportunity for the vendor involved in the appeal to make its case.*
2. That a mechanism for publishing decisions and clarifications from NASED be established and be made widely known.

Required and Optional Functions

There are conflicting words throughout this draft about which functions are required and which are optional. Volume I, section 1.6 says:

> *"Standards are mandatory requirements and are designated by use of the term "shall."*

Volume I, section 2 uses the word "shall" for every item. But volume II, section 2.3.a says (note the underlined words):

> *"The vendor shall organize the presentation of required capabilities in a manner that corresponds to the structure and sequence of functional capabilities indicated in Volume I, Section 2 of the Standards. The contents of Volume I Section 2 may be used as the basis for a checklist whereby the vendor indicates the specific functions provided and those not provided by the system."*

Off The Shelf Hardware

Commercial Off The Shelf (COTS) hardware. There are numerous inconsistencies in how the proposed standards address COTS hardware:

Overview, page 6:

> *These devices and software are exempted from certain portions of the qualification testing process so long as such products are not modified in any manner for use in a voting system.*

Vol 1, 1.6:

> *Some voting systems use one or more readily available commercial off-the-shelf (COTS) devices (such as card readers, printers, or personal computers) or software products (such as operating systems, programming language compilers, or database management systems). COTS devices and software are exempted from certain portions of the*

qualification testing process as defined herein, as long as such products are not modified for use in a voting system.

Vol 1, 3.1.1:

The requirements of this section apply generally to all hardware used in voting systems, including: ... b. Hardware furnished by an external provider (for example, providers of commercial off-the-shelf (COTS) machines and devices) where the hardware may be used in any way during voting system operation;

Vol 1, 3.4.6:

These procedures will be applied to all devices for casting, scanning and counting ballots, except those that constitute COTS devices that have not been modified in any manner to support their use as part of a voting system and that have a documented record of performance under conditions defined in the Standards.

Vol 1, 9.3.1:

COTS hardware, system software and communications components with proven performance in commercial applications other than elections, however, are exempted from certain portions of the test as long as such products are not modified for use in a voting system.

Vol 2, 4.2.1:

All hardware components custom-designed for election use shall be tested in accordance with the applicable procedures contained in this section. Unmodified COTS hardware will not be subject to all tests. Generally such equipment has been designed to rigorous industrial standards and has been in wide use, permitting an evaluation of its performance history. To enable reduced testing of such equipment, vendors shall provide the manufacturers specifications and evidence that the equipment has been tested to the equivalent of the Standards.

Vol 2, 4.6.1:

Systems exclusively designed with system-level COTS hardware whose configuration has not been modified in any manner and are not subjected to this segment of hardware testing.

Vol 2, 4.7.1:

COTS hardware, as defined previously, may not be subjected to the 48-hour chamber segment of the operating environmental tests.

Vol 2, Appendix A, 4th paragraph of the introduction:

It is also specified by the standards that voting systems incorporating the vendor's software and off-the-shelf hardware need only be submitted for software and system-level tests.

It is our recommendation that the words of Vol 2, section 4.2.1, especially the last sentence, be adopted throughout these standards.

SEQUOIA
voting systems

Coding Standards

Volume I, Section 4.2 has changed significantly since the first draft of the standards. It now contains numerous prescriptive, restrictive and sometimes archaic requirements. It is also excessively targeted to the C and C++ languages. As a whole it contradicts Volume 1, Section 4.1, where it is said:

> *This section recognizes that there is no single "best" way to design software. Many programming languages are available for which modern programming practices are applicable, such as the use of rigorous program and data structures, data typing, and naming conventions. Other programming languages exist for which such practices are not easily applied.*

And also section 1.1, where it is said:

> *"The Standards address what a voting system should reliably do, not how the system should meet these requirements."*

We object in the strongest possible way to the inclusion of Volume I, Section 4.2 as written, and urge that the text from the first draft be used instead.

That no documents are cited in Appendix B to support the demands of this section is at best curious; shall an entire industry be held hostage by one code reviewer's opinions? That is the case with the words that have been written here.

The various flowcharted items, such as how a loop works, are best moved to a "Software Design Tutorial" Appendix, if it is the desire of these standards to provide a basic software engineering education.

Finally, Volume II, section 5.4, has a well written set of guidelines that can and should be applied to voting systems. These guidelines are just as comprehensive, but avoid the narrow-mindedness and technology-specific nature of Volume I, Section 4.2.

Volume 1 Specific Notes

Typographical Errors

2.4.3.2.2. "underrate" should be "undervote".
2.4.3.2.2.k. Missing the word "ballot" 4 words from the end.
5.3, top of last page. Change "telecommunications if prohibited" to "telecommunications is prohibited".

Specific notes

Section 1.4. It is unclear as to whether ADA compliance is optional or required. Especially in light of various Vol II words, such as Vol II, section 6.5.

SEQUOIA
voting systems

Section 1.5.4. It appears impossible to reconcile this section with section 5.3, where it is stated:

> *"the transmission of data using telecommunications if prohibited for the following data types: ... f. Official election results (from the polling place to central office of the jurisdiction)"*

Section 2.2. This section says in part "all voting systems shall provide .... Telecommunications". Is it the intent of the FEC to not longer certify systems that use the physical transport of results from polling place to the count center?

More specifically, since Vol I, Section 5.3 prohibits the use of telecommunications for just about every useful purpose, it would be good to explain in these standards the allowable purposes for this required telecommunications capability.

Section 2.2. If all systems must provide the list of functions shown, (i.e. Election Management System), the distinction between hardware/firmware ITA and software ITA becomes a thing of the past. It will not be possible to certify just a voting machine, or just an election management system. Are Wyle, Ciber and Systest prepared for this?

Section 2.2.4.1. It would be wise to enhance this requirement with a prohibition of any system that has a single point of failure that would prevent further voting at the polling place, by a means compatible with these standards.

Section 2.2.7.1.c. "...have a height between 15 inches maximum and 46 Inches...". It appears that the word "maximum" is misplaced.

Section 2.2.7.2. Why are only DRE systems required to provide access to voters with disabilities? In light of current events, it would seem a mistake to make this distinction.

Section 2.2.7.2.b.8: Is the intent to have a maximum volume adjustable up to 105 dB or one that cannot go higher than 105 dB, but that does not have to go to 105 dB? This is significant not only because 105 dB is deafeningly loud, but because the proposed Florida Voting System Standards specify a maximum volume of 97 dB. It would be perhaps clearer to state what the maximum and minimum volume ranges must be.

Section 2.2.10. This section is in conflict with the prohibitions listed in section 5.3.

Section 2.4.2.a. This section uses the term "ballot image" to mean the visual ballot shown to the voter. This is in conflict with the definition of the term.

SEQUOIA
voting systems

Section 2.4.2.a. Does this section intend to prohibit existing full-face DRE equipment that uses a paper overlay on a grid of buttons? Please consider the implications of such a ban on New York State, where by law only a full-face ballot presentation is allowed. Does the FEC intend to consign New York to only use lever machines?

Section 2.4.3.1.a. This paragraph indicates that "all systems" must have the capability of magnifying the font size to 18 point. Is it acceptable for paper based systems to use a magnifying lens to satisfy this requirement? If so, then the same should be the case for DRE systems.

Section 2.4.3.3. Is it the intent that every item listed here be required, with no ability for jurisdiction control? In particular, (e) which requires an indication of undervoting, and (i), which requires an "are you sure" before casting the ballot, have the potential to make the voting process much slower and complex for 99% of the population.

Section 2.4.3.3.i Is it the intent of this paragraph to require some sort of "are you sure" prompt?

Section 2.4.3.3.k Providing a clear indication of a problem is a good thing, but is giving the voter the instructions on how to proceed best? At this point, since there has been a failure, intervention by a pollworker seems called for. We suggest the following replacement wording:

> "Notification that the ballot has not been cast successfully, and clear instruction as to the steps the voter should take to cast his or her ballot should this event occur;"

Section 2.4.3.3.l. A 10 second response time is much too slow for a system designed for the general public. 1 second is much more appropriate.

Section 2.4.3.3.o. Incorrect section reference (should be 2.2.2.2, not 2.2.2.2.2).

Section 2.4.3.3.o. A definition of "human readable" should be included, as an electronic memory device, whether storing text or binary data, is not human readable without the intervention of some form of reading or printing software.

See also section 3.2.4.3.2.c.3, where encoding and compression of the ballot image data is permitted. This is inconsistent with requiring a human-readable format.

Section 2.5.1.e. It should never be possible to reopen polls on DRE systems, under any circumstance.

Section 3.2.4.3.2.b. This appears to require multiple memory devices in any removable memory device. Is this the intent? Are multiple storage locations within a single device (i.e. PCMCIA card) no longer acceptable?

Section 3.4.8. As defined by the FCC, electronic equipment used in an office environment is required to be compliant with part 15, class A. Therefore, the appropriate limit for central count equipment is Class A.

Section 3.4.18.b. This sentence appears to require disabled access for all possible users, including pollworkers and technicians. Is this the intent?

Section 4.2.3.c. Why is code from commercial code generators exempt from the line length limit?

Section 4.2.6.a. This is fine for general purpose desktop software, but imposes an unnecessary performance and code bloat burden on embedded systems, where the validity of arguments is much more tightly controlled.

Section 4.2.6.e. and 4.2.6.f. say the same thing.

Section 4.2.6.m. First word should be "Initialize", not "Initialized".

Section 4.2.6.l and 4.2.6.n. Given the use of C as the model for the coding constructs within other parts of section 4.2.6, the if statements here should be corrected to use the equality (= =) operator instead of the assignment (=) operator. See also 4.2.6.e.

Section 4.2.6.r. Asking the code reviewer to also be an expert on spelling and grammar is unrealistic. How does this rule intend to accommodate abbreviations? Displays that have a limited size, such that grammatically correct sentences cannot be formed? This section, if it even belongs in the standards, is better placed in Volume II, and should refer to user documentation. If this section is to remain, given the complexity of the English language, references must be cited, so the industry is not burdened by one person's opinions. If this requirement is to be part of the standards, it is better placed as part of section 2.2.5.2.

Section 4.2.8. This says in part *"Software changed in any way must adhere to these standards"*. This needs clarification as to the scope. As an actual example, suppose an existing, public-domain implementation of DES is adopted. Many such exist, and while well written, do not conform to the draconian requirements proposed here. Suppose further that this public domain code is modified to use a header structure and #include

file consistent with the rest of the code. Would such a change require the *entire* module to become compliant?

Section 5.3. By the definition of telecommunications in previous sections, there appears to be prohibitions on the following:

1. Modem transmissions from polling places of vote data, when polls close.
2. The use of client/server type systems (networked) for loading ballot definition data onto voting machines, and for election night consolidation of vote data.

Section 6.1.2. The first draft included the following very important category:

> *Software that operates on voting devices (such as personal computers) under the control of individual voters and third persons other than the voting jurisdiction (e.g., employer, library, hotel, college) for use by the voter, such as for Internet voting systems.*

To meet the stated goals of secure reliable voting systems, this must be reinstated.

Section 7.1.f. This existed in the original release, but has been deleted. Why?

Section 7.6. Does not exist in this draft. Why?

Volume 2 Specific Notes

Typographical Errors

Page 2-6, at the bottom: "osverview"
Page 2-7, last line: "operate of system"
Many instances: "Lightening" involves making something less dark. "Lightning" is what thunderstorms produce.
Page 2-9, last sentence: insert "that" between "other items" and "provide data"
Page 2-12. Missing period at very end.
Page 2-15, first sentence of 2.5.9.1: Delete "provide"
Page 2-17. Section 2.5.9.d has two subparts 3).
Page 3-1. Section 3.2.1. Words missing between "test procedures" and "a voting system".
Page 3-1. Section 3.2.1. First word of second sentence should be "Test".
Page 4-7. Section 4.6.2. Last step should not be "Step X".
Page 4-9. Section 4.6.6. This is the humidity test, not high temperature.
Page 4-10. Section 4.6.6.2. Last step should be step 9.

SEQUOIA
voting systems

Specific notes

Section 2.1.1.1. Paragraph at the end needs to delineate "developmental" documentation. What exactly is not required for already-certified systems? All TDP items, or just certain ones?

Section 2.2.2 Is a block of text missing after the first sentence?

Section 2.2.2. What is the purpose of providing the performance information? There is nothing anywhere that defines criteria for the acceptability of such.

Section 2.5.3. Is it acceptable to procure software items from a reseller or distributor? For example, is it even possible for a small vendor to purchase direct from Microsoft?

Section 2.5.5.2. Last sentence. Can this requirement be better explained?

Section 2.5.7.g. Is the section reference included here correct?

Section 2, overall. Many of the documents descriptions conclude with a list of suggested/recommended appendices. Many suggested topics are duplicated, which invites problems of revision control. Would it be safer to provide each appendix topic but once, and have other documents cross-reference it?

Section 2.8.7.c. "Every conceivable faulty operator input"? This hardly seems practical.

Section 3.1. A mention is made of testing for internet-based systems, yet nothing exists later in section 3 on this topic.

Section 4.6.1. The second paragraph, referring to COTS hardware, conflicts with section 4.2.1. Section 4.2.1, exempts COTS hardware only if testing equivalent to the FEC spec can be documented. This is the appropriate requirement, as it refuses a blanket exemption to low-reliability consumer-grade electronics, such as personal computers.

Section 4.6.1.2. This section mixes up the configurations for storage, shipping, and transport to the polling place. It is possible that the three are identical, but not likely (i.e. an additional cardboard box for common-carrier shipping). It is also not appropriate to configure the equipment in any of these configurations for the bench handling test of 4.6.2.

Section 4.6.2 Last step refers to removing the unit from the transit case, even though it was not in such.

SEQUOIA
voting systems

Section 4.6.4. A low temp of –4F is insufficient to account for unheated warehouses. This limit should be –20F.

Section 4.7.1. The last paragraph indicates that the "software need only operate to the extent necessary to enable the identification of hardware failures". This seems to be in conflict with 4.7.2, where the equipment is actively processing votes during the test.

Section 4.7.1. The last sentence conflicts with the COTS limited exemption of section 4.2.1.

Section 4.7.4. The appropriate limit for central count equipment is FCC Class A.

Section 4.7.11.a. Is something missing from this paragraph?

Section 4.7.14. This is a far too low an MTBF value. In a typical election, a precinct count machine would be operated for at least 16 hours (setup time, plus in-precinct time). With a 163 hour MTBF, this equates to 1 out of 10 machines failing in each election. This is unacceptably high by at least a factor of 10. This number is appropriate to central count equipment only.

Section 5.4. This is a well written yet flexible set of guidelines for producing maintainable and robust software, versus the archaic and limiting absolute requirements of volume I, section 4.2.

Section 6.2.3. The requirement that all testing be done with ballots of the maximum length places undue burdens on qualifying systems where the ballot length has no practical limit (i.e. limited by memory size only).

Section 6.5. It appears from this section that ADA compliance is optional. This is in contrast to volume I, and volume II, section 3.4, where it appears required for all systems.

Section 6.6.c. What is the definition of "standard" as used in the first sentence? Different than "COTS", as used elsewhere?

Section 6.6.e. "All changes to the system hardware that may produce a change in software operation shall also be subject to reexamination". Question 1: Does this include changes in COTS components? Question 2: Who determines what "may" produce a change in operation?

SEQUOIA
voting systems

Appendix A. Paragraph 4, sentence 2 conflicts with other places where COTS hardware is mentioned.

C.4. Last bullet point: The number in parenthesis, 3,126,404 is not consistent with the rest of the section. To follow the main text, there would be a total of between (26,997 + 1,576,701) and (1,549,703 + 1,576,701) reads with one error.

C.5. The inputs chosen for the equations are numbers such as 5% or 95%. These are numbers with 1 or 2 significant figures. Yet the numbers that result are given with up to 7 significant figures. This is unreasonable, as anyone who has used a slide rule should remember. Suggest revising numbers as shown:

1,549,703 → 1,550,000
26,997 → 27,000
1,576,701 → 1,580,000